CLAIMS

WHAT IS CLAIMED IS:

1. A security system for controlling access to encrypted information, comprising:

a hardware device for storing at least one decryption key for use in decrypting an encrypted item of information, the decryption key being associated with a security code which is used by the hardware device to determine whether it is authorized to send encrypted copies of the decryption key to others.

2. The security system of claim 1, wherein if the hardware device is authorized to send an encrypted copy of the decryption key to a first entity, it encrypts the decryption key using an encryption key associated with the first entity.

3. The security system of claim 2, wherein the decryption key is encrypted with a public key of the first entity.

4. The security system of claim 1, wherein each time the hardware device sends a decryption key to another entity, it modifies the security code associated with the decryption key and sends the modified security code as part of the encrypted decryption key.

5. The security system of claim 4, wherein the security code is a numeric value indicating the number of times the encryption key can be propagated, and the security code is decremented each time the decryption key is propagated to a further entity.

6. The security system of claim 1, wherein the decryption key is stored within the hardware device.

7. The security system of claim 1, wherein the hardware device is removable from a data processor.

8. The security system of claim 1, wherein the hardware device is in the form of a user unit, that a user introduces to a data processor when the user wishes to use the data processor to access encrypted information and removes the user unit from the data processor when the user has finished.

9. The security system of claim 1, wherein each time the hardware device propagates a decryption key, it includes as part of the decryption key an identifier indicating the identity of a sender's key.

10. The security system of claim 9, wherein the decryption key includes an audit trail of individuals who have allowed propagation of the key.

11. The security system of claim 9, wherein a user can append a control word against their identity in the decryption key to instruct the hardware device to initiate a message to them or an agent informing them of the propagation of the key and giving information concerning that propagation.

12. The security system of claim 1, wherein the decryption key is passed between a plurality of hardware devices.

13. The security system of claim 1, wherein a user's private key is stored within their own hardware device, such that the encrypted decryption key can only be decrypted when the hardware device is in operation.

14. The security system of claim 1, wherein the hardware device includes a data processor such that all encryption and decryption of the decryption keys is performed within the hardware device.

15. A method of controlling propagation of a decryption key that allows access to encrypted data, the method comprising the steps of:

associating a propagation control word with the decryption key for an item of data, and in response to an instruction to send the key to a specified recipient, checking the status of the control word to determine if propagation is allowed, and if so, modifying the control word and encrypting the control word and decryption key with a recipient's public key and sending the encrypted key.

16. The method of claim 15, wherein the control word is a numeric value which is decremented at each propagation, and wherein propagation is inhibited once the numeric value reaches a predetermined value.

17. The method of claim 15, wherein an originator of the decryption key sets a maximum number of times the key can be sent, and each time the key is sent, a variable holding a generation number of the key is modified such that when the generation number reaches the maximum number of times the key can be sent, further sending of the key is inhibited.